AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of protecting a cryptographic algorithm (6) before introduction in an enciphering device (1) comprising programmable processor unit (4), the algorithm being separable into the form of initial polynomials (P_i) of at least two variables each, and having a degree of not less than two, the method comprising: ~~the steps of~~

providing to the enciphering device at least two initial polynomials (P_j, P_{j+1});

combining, on the enciphering device, combined polynomials (Q_k), each obtained from the at least two initial polynomials (P_i, P_{i+1}); and ~~of~~

implementing the combined polynomials (Q_k) in the programmable processor unit (4).

2. (Currently Amended) A method according to claim 1, further comprising: ~~the step of~~ storing the combined polynomials (Q_k) in the form of a configuration file that is loaded into a memory (3) associated with the processor unit (4).

3. (Previously Presented) A method according to claim 2, wherein the memory (3) and the programmable processor unit (4) are associated with an eraser member (5) serving, in the event of an intrusion into the device, to erase the processor unit (4), and to erase the memory (3) containing the configuration file when the configuration is present in said memory.

4. (Currently Amended) A method according to claim 1, further comprising: ~~including the step of~~

combining each combined polynomial (Q_k) with a function (f_k)[[,]]; and ~~of~~

KM/JAV

combining the following combined polynomial (Q_{k+1}) with an inverse function (f_k^{-1}).

5. (Previously Presented) A method according to claim 4, wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

6. (New) An enciphering device which utilizes a cryptographic algorithm, comprising:

a programmable processor unit;

an eraser member coupled to the programmable processor unit; and

a memory coupled to the eraser unit and the programmable processor unit, wherein the cryptographic algorithm is protected prior to its introduction into the enciphering device, and

further wherein the cryptographic algorithm is separable into the form of initial polynomials (P_i) of at least two variables each, having a degree of not less than two, and

further wherein the programmable processor unit receives the initial polynomials (P_i, P_{i+1}), and combines the at least two initial polynomials (P_i, P_{i+1}) to form combined polynomials (Q_k).

7. (New) The enciphering device according to claim 6, wherein the combined polynomials (Q_k) are stored in the form of a configuration file that is loaded into the memory.

8. (New) The enciphering device according to claim 7, wherein in the event of an intrusion into the enciphering device, the eraser member will erase the processor unit and memory containing the configuration file when the configuration is present in said memory.

KM/JAV

9. (New) The enciphering device according to claim 6, wherein each combined polynomial (Q_k) is combined with a function (f_k), and the following combined polynomial (Q_{k+1}) is combined with an inverse function (f_k^{-1}).

10. (New) The enciphering device according to claim 9, wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

KM/JAV